ATTACHMENT A

TiVo Approach To Receiver Robustness

TiVo provides a service to its subscribers that has many of the properties of a secure content broadcasting service:

The company must validate that any TiVo receiver is known, still believed secure, and is due service.
The TiVo receiver must validate that the service it is contacting is known and trusted.
Data delivered to a TiVo receiver by the service must be secure and trusted.
Usage logging information uploaded by the receiver must be secure in order to protect the privacy of the viewer.
The TiVo Service must be able to enable or disable specific services on the receiver in a secure and reliable manner.
Content stored on the local disk drive in the receiver must be encrypted uniquely to that receiver, and the encryption keys for that content must themselves be secure.

These goals parallel and exceed those for a demodulator. They are accomplished within the receiver without the drawbacks of the "bank vault" robustness method suggested by the Proposed Regulations. The technique used by TiVo relies instead on insuring that the receiver never executes untrusted software. This is accomplished by following the "chain of trust": A secure, embedded ROM, epoxyed to the mainboard is responsible for loading an operating system kernel, and checking that the kernel has not been tampered with, using the public signing key for the TiVo Service. If the kernel is valid, it is given control of the system, at which point it performs the same validation on all operational software and files. If this step succeeds, it is known that all software in the receiver is valid and trusted, and normal operation begins. Otherwise, the receiver fails to start.

During operation, the software relies on a separate security microprocessor to hold a dedicated secret key for that receiver. The operational software relies on this microprocessor for strong encryption operations. The software in this microprocessor is "burned in", inhibiting changes, and it will not disclose the secret key. In combination with a trusted software environment, it becomes possible to reliably encrypt and decrypt content, to securely manage encryption keys, and handle inter-device communication.

The properties of this approach, now running reliably in hundreds of thousands of TiVo receivers, are:

All encryption algorithms used are well-tested and in the public domain.
The operation of the secure software does not need to be obscured in any way. The software itself may be examined freely and with any tools desired.
There are no "global secrets" to disclose that can compromise other receivers.
Compromising the operation of the receiver requires replacing the boot ROM, a challenging operation for the most skilled, and prone to mistakes.

The disk may be removed and placed in a PC, but the content will not be readable. TiVo is able to design and debug receivers with relative ease, and offer the lowest possible price to the consumer.

Thus, the TiVo approach provides security at least as good or better than the "bank vault" approach, while granting other advantages such as lower cost to manufacture. In approaching a definition of demodulator robustness for unencrypted content, TiVo therefore urges the Commission to consider a simpler requirement by specifying:

"Covered Demodulator Products shall be manufactured in a manner that provides sufficient mechanisms to assure that unauthorized modifications of operational software are possible only by direct modification of trusted hardware components, such modifications being beyond the capability of the ordinary user, using commonly available tools, and likely to damage the device."

This definition encompasses the “TiVo approach” as well as the "bank vault" approach, should a manufacturer wish to pursue that path.

Normal
Normal
Default Paragraph Font
Default Paragraph Font
Inside Address
Inside Address
Footnote Text
Footnote Text
Footnote Reference
Footnote Reference
Body Text 2
Body Text 2
Header
Header
Footer
Footer
Subtitle
Subtitle
Matt ZinnOC:\Documents and Settings\mattz\Desktop\TiVo Ex Parte 10-3-03 Attachment A.doc Matt ZinnBS:\FCC\Broadcast flag\TiVo Letter 02-230 10-3-03

Attachment A.doc Matt ZinnBS:\FCC\Broadcast flag\TiVo Letter 02-230 10-3-03
Attachment A.doc
Matt ZinnOC:\Documents and Settings\mattz\Desktop\TiVo Ex Parte 10-3-03
Attachment A.doc Matt ZinnBS:\FCC\Broadcast flag\TiVo Letter 02-230 10-3-03
Attachment A.doc Matt ZinnBS:\FCC\Broadcast flag\TiVo Letter 02-230 10-3-03
Attachment A.doc
Unknownÿ□
Times New Roman
Times New Roman
Symbol
Symbol
Wingdings
Wingdings
Courier New
Courier New
.An alternative approach has been taken by TiVo
.An alternative approach has been taken by TiVo
Matt Zinn Matt Zinn
Matt Zinn Matt Zinn
discovery
discovery
An alternative approach has been taken by TiVo
Matt Zinn
Normal
Matt Zinn
Microsoft Word 9.0
TiVo, Inc.
An alternative approach has been taken by TiVo
Root Entry
1Table
1Table
WordDocument
WordDocument
SummaryInformation
SummaryInformation
DocumentSummaryInformation
DocumentSummaryInformation
CompObj
CompObj
ObjectPool
ObjectPool
Microsoft Word Document
MSWordDoc
Word.Document.8